Available online at www.sciencedirect.com
ScienceDirect
Linear Algebra and its Applications 418 (2006) 591–594
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

Even poset and a parity result for binary linear code

Yaokun Wu

Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, China

Received 23 January 2006; accepted 20 February 2006
Available online 21 April 2006
Submitted by R.A. Brualdi

Abstract

Let $\mathscr{C}$ be a linear binary code, namely a subspace of the space consisting of all binary vectors of a fixed length. A vector in $\mathscr{C}$ is maximal provided it has a maximal support among $\mathscr{C}$; a nonzero vector in $\mathscr{C}$ is minimal provided it has a minimal support among $\mathscr{C} \setminus \{0\}$. We prove that the sum of all maximal vectors of $\mathscr{C}$ equals the sum of all minimal vectors of $\mathscr{C}$. In course of this research, we introduce the concept of even poset and establish a duality result for it.

AMS classification: 05C45; 06A06; 15A03

Keywords: Support; Eulerian graph; Binary matroid; Minimal vector

1. Even poset

Let $P = (X, \leqslant)$ be a poset. For any $x \in X$, we define $\downarrow x = \{y \in X : y \leqslant x\}$ and $\uparrow x = \{y \in X : y \geqslant x\}$, and call them a principal ideal and a principal filter of P, respectively [6, p. 20]. Note that x is maximal in P if and only if $|\uparrow x| = 1$ whereas x is minimal in P if and only if $|\downarrow x| = 1$. We say that P is an even poset provided every principal ideal or principal filter of it either has size 1, and hence corresponds to a minimal or maximal element of P, respectively, or has an even size. For any natural number n, $[n]$ stands for $\{1, \dots, n\}$.

E-mail address: ykwu@sjtu.edu.cn

0024-3795/$ - see front matter
doi:10.1016/j.laa.2006.02.028

Example 1. Let n, m be two natural numbers. Let $\Theta_{n,m} = \{(A_1, A_2, \ldots, A_m) : A_i \subseteq [n], A_i \cap A_j = \emptyset, \forall i \neq j\}$ and order it by setting $(A_1, A_2, \ldots, A_m) \leqslant (B_1, B_2, \ldots, B_m)$ if and only if $A_i \subseteq B_i$ for all $i \in [m]$. It is easy to see that the resulting poset is an even poset provided m is odd.

Lemma 2. *For each finite even poset, the number of its maximal elements and the number of its minimal elements have the same parity.*

Proof. Let $P = (X, \leqslant)$ be the given even poset and $\mathscr{M}(P)$ and $\mathrm{M}(P)$ be its sets of maximal elements and minimal elements, respectively. The result is straightforward from the following double counting reasoning:

$$|\mathscr{M}(P)| = \sum_{x\in\mathscr{M}(P)} 1 \equiv \sum_{x\in X}\sum_{y\geqslant x} 1 = \sum_{y\in X}\sum_{x\leqslant y} 1 \equiv \sum_{y\in \mathrm{M}(P)} 1 = |\mathrm{M}(P)| \pmod 2. \qquad \square$$

2. Binary linear code and its support poset

Consider the linear space $V = \mathbb{F}_2^n$ consisting of $1 \times n$ vectors over the binary field $\mathbb{F}_2$, which can be viewed as $\mathbb{F}_2^{[n]}$, the set of functions from $[n]$ to $\mathbb{F}_2$. Let W be a subspace of V, which is called a binary linear code in coding theory. Each $w \in W$ is uniquely determined by its support, denoted $\mathbf{supp}(w)$. For any $X \subseteq V$, let $\mathscr{S}(X) = \{\mathbf{supp}(w) : w \in X\}$. The support poset of W is $\mathscr{S}(W)$ ordered by the inclusion relation and we will simply refer to it also by $\mathscr{S}(W)$. For any $A \subseteq [n]$, the subposet $\mathscr{S}_A(W)$ of $\mathscr{S}(W)$ is defined to be $\{B \in \mathscr{S}(W) : A \subseteq B\}$ and the notation W_A is used to denote $\{w \in W : w(i) = w(j), \forall i, j \in A\}$.

For $A \subseteq [n]$ and $w \in \mathbb{F}_2^{[n]}$, we define $p_A(w)$ to be the element of $\mathbb{F}_2^A$ with $\mathbf{supp}(p_A(w)) = \mathbf{supp}(w) \cap A$. Put $p_A(W) = \{p_A(w) : w \in W\}$ and $q_A(W) = \{p_A(w) : w \in W, \mathbf{supp}(w) \subseteq A\}$.

Recall that binary linear code, binary clutter and binary matroid are three equivalent structures [5,8]. We point out that p_A and q_A just correspond to the contraction operation and the deletion operation in matroid theory, respectively. Considering the important role played by the contraction/deletion operation in matroid theory, it is natural that they appear in the study of binary linear code [7,15].

3. A parity result for binary linear code

Lemma 3. *For any binary linear code $W \leqslant \mathbb{F}_2^n$ and any $A \subseteq [n]$, $\mathscr{S}_A(W)$ is an even poset.*

Proof. Take, if any, a $B \in \mathscr{S}_A(W)$ which is neither maximal nor minimal in $\mathscr{S}_A(W)$. Our task is to show that both the principle filter $\uparrow B$ and the principal ideal $\downarrow B$ in $\mathscr{S}_A(W)$ have an even size.

Observe that $\uparrow B$ is just $\{C \cup B : C \in \mathscr{S}(q_{[n]\setminus B}(W))\}$. This tells us that it has equal size with the binary linear subspace $q_{[n]\setminus B}(W)$. But, as B is not maximal, $q_{[n]\setminus B}(W)$ is of positive dimension and thus has an even size.

We now consider $\downarrow B$. If $A = \emptyset$, then we find that $\downarrow B$ is just $\mathscr{S}(q_B(W))$. Since B is not minimal, $\mathscr{S}(q_B(W))$ is a binary space of positive dimension and so has an even size. For the remaining case $A \neq \emptyset$, we can check that the binary linear space $\mathscr{S}(q_B(W_A))$ is a disjoint union of $\downarrow B = \{C \in \mathscr{S}(q_B(W_A)) : A \subseteq C\}$ and $Z = \{C \in \mathscr{S}(q_B(W_A)) : A \cap C = \emptyset\}$. But the map sending C

to $B \setminus C$ obviously induces a bijection from $\downarrow B$ to Z. This yields that $|\downarrow B| = \frac{|\mathscr{S}(q_B(W_A))|}{2}$. In light of the fact that B is not minimal in $\mathscr{S}_A(W)$, the dimension of $q_B(W_A)$ has to be greater than one. Consequently, we conclude that $|\downarrow B|$ is even, ending the proof. □

Combining Lemmas 2 and 3, we get the following parity result for a linear binary code. We mention that it is equivalent to what we announce in the abstract, as can be seen by picking $\mathscr{C} = W_A$.

Theorem 4. *For any $W \leqslant \mathbb{F}_2^{[n]}$ and $A \subseteq [n]$, the number of maximal elements in $\mathscr{S}_A(W)$ and the number of minimal elements in $\mathscr{S}_A(W)$ have the same parity.*

4. Applications

Consider a subspace W of $\mathbb{F}_2^n$. Let $\mathscr{S}'(W)$ be the truncated support poset of W, which is obtained from $\mathscr{S}(W)$ by removing its bottom element, namely $\emptyset$. Say that $w \in W$ is maximal if $\mathbf{supp}(x)$ is a maximal element in $\mathscr{S}(W)$ [2]. Say a nonzero vector $w \in W$ is minimal if $\mathbf{supp}(w)$ is minimal in $\mathscr{S}'(W)$ [1,3]. We write $\mathsf{M}(W)$ and $\mathsf{m}(W)$ for the set of maximal and minimal vectors of W, respectively.

Taking $A = \emptyset$ in Theorem 4, we deduce Hoffmann's Theorem.

Corollary 5 [9]. *For any subspace W of $\mathbb{F}_2^n$, we have $|\mathsf{M}(W)|$ is odd.*

Letting A run through all singleton sets of $[n]$ in Theorem 4, we come to the next corollary. As commented preceding Theorem 4, it is an equivalent form of Theorem 4.

Corollary 6. *For any $W \leqslant \mathbb{F}_2^n$, it happens that $\sum_{x\in \mathsf{m}(W)} x = \sum_{x \in \mathsf{M}(W)} x$.*

To present a real application of Theorem 4, we will resort to a mathematical result underlying the so-called 'Lights Out Game' [4,16]. For the sake of completeness, we derive here a direct generalization of this result for our use.

Lemma 7. *Let A be an $n \times n$ matrix over a field $\mathbb{F}$ and $u \in \mathbb{F}^n$. If $u^\top u - A$ is skew-symmetric and has all zeros on its diagonal, then there is $x \in \mathbb{F}^n$ such that $xA = u$.*

Proof. Denote the row space of A by $\mathscr{C}$. Note that $\mathscr{C} = (\mathscr{C}^\perp)^\perp$. Accordingly, it suffices to show that for any $w \in \mathscr{C}^\perp$ we have $uw^\top = 0$, or equivalently $wu^\top uw^\top = 0$. To see this, first observe that $w \in \mathscr{C}^\perp$ implies $Aw^\top = 0$. Moreover, we get from our assumption on $u^\top u - A$ that $w(u^\top u - A)w^\top = 0$. By now, the lemma follows from $wu^\top uw^\top = w(u^\top u - A)w^\top + wAw^\top$. □

Corollary 8. *Let A be an $n \times n$ symmetric matrix over $\mathbb{F}_2$ whose diagonal is occupied by all ones. Let W be the row space of A. Then $\sum_{x\in m(W)} x$ is the vector of all ones.*

Proof. Take u to be the vector of all ones. It is immediate from Corollary 6 that $\sum_{x\in \mathsf{m}(W)} x = u$ if and only if $u \in \mathsf{M}(W)$. But the fact that $u \in W$, and hence $\mathsf{M}(W) = \{u\}$, is guaranteed by Lemma 7, as was also proved in [4,16]. This is the proof. □

5. Conclusion

Theorem 4 is motivated by a series of earlier work on characterizing Eulerian graphs, bipartite graphs and, more generally, Eulerian and bipartite binary matroids [7,9–15,17–20]. Almost all earlier work along this line make use of some inductive arguments. We notice that for the 'short' proofs along the approach of McKee [10,11], some careful arguments have to be incorporated to make them more complete. The key to our work is the introduction of the concept of even poset.

We remark that all posets mentioned in this note are graded and has the same number of elements of even rank as odd rank in every interval of positive length.

It is clear that this property and the property of being an even poset are both invariant under the Cartesian product operation. Thus, a natural question to consider is to figure out the relationship between even posets and posets with the above-mentioned property. In general, we would like to know to which extent we can determine (classify) all even posets.

Acknowledgements

Thanks are due to Herbert Fleischner, Terry A. McKee, Jian Shen, Maruti M. Shikare, and Douglas R. Woodall for their help in providing relevant references. This work is supported by the NNSFC grant 10301021.

References

[1] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inform. Theory 44 (1998) 2010–2017.
[2] Y. Borissov, N. Manev, S. Nikova, On the non-minimal codewords in binary Reed-Muller codes, Discrete Appl. Math. 128 (2003) 65–74.
[3] Y. Borissov, N. Manev, Minimal codewords in linear codes, Serdica Math. J. 30 (2004) 303–324.
[4] Y. Caro, Simple proofs to three parity theorems, Ars Combin. 42 (1996) 175–180.
[5] G. Cornuéjols, Combinatorial Optimization: Packing and Covering, SIAM, Philadelphia, 2001.
[6] B.A. Davey, H.A. Priestley, Introduction to Lattices and Orders, second ed., Cambridge University Press, Cambridge, 2002.
[7] H. Fleischner, Elementary proofs of (relatively) recent characterizations of Eulerian graphs, Discrete Math. 24 (1989) 115–119.
[8] J.C. Fournier, Binary matroids, in: N. White (Ed.), Combinatorial Geometries, Cambridge University Press, Cambridge, 1987, pp. 28–39.
[9] P. Hoffmann, Counting maximal cycles in binary matroids, Discrete Math. 162 (1996) 291–292.
[10] T.A. McKee, Recharacterizing Eulerian: intimations of new duality, Discrete Math. 51 (1984) 237–242.
[11] T.A. McKee, *S*-minimal unions of disjoint cycles and more odd Eulerian characterizations, Congressus Numeran. 177 (2005) 129–132.
[12] T.T. Raghunathan, M.M. Shikare, B.N. Waphare, Splitting in a binary matroid, Discrete Math. 184 (1998) 267–271.
[13] M.M. Shikare, G. Azadi, Determination of the bases of a splitting matroid, Eur. J. Combin. 24 (2003) 45–52.
[14] M.M. Shikare, New characterizations of Eulerian and bipartite binary matroids, Ind. J. Pure Appl. Math. 32 (2001) 215–219.
[15] M.M. Shikare, T.T. Raghunathan, A characterization of binary Eulerian matroids, Ind. J. Pure Appl. Math. 27 (1996) 153–155.
[16] K. Sutner, Linear cellular automata and the Garden-of-Eden, The Math. Intell. 11 (1989) 49–53.
[17] S. Toida, Properties of a Euler graph, J. Franklin Inst. 295 (1973) 343–345.
[18] D.J.A. Welsh, Eulerian and bipartite matroids, J. Combin. Theory B 6 (1969) 357–377.
[19] P.J. Wilde, The Euler circuit theorem for binary matroid, J. Combin. Theory B 18 (1975) 260–264.
[20] D.R. Woodall, A proof of McKee's Eulerian-bipartite characterization, Discrete Math. 84 (1990) 217–220.